INTERNET OF THINGS

UNIT-1
Introduction to IOT

Definition and Characteristics of IoT – IoT Architectures-Challenges and Issues - Physical Design of IoT, Logical Design of IoT - IoT Functional Blocks, Security.

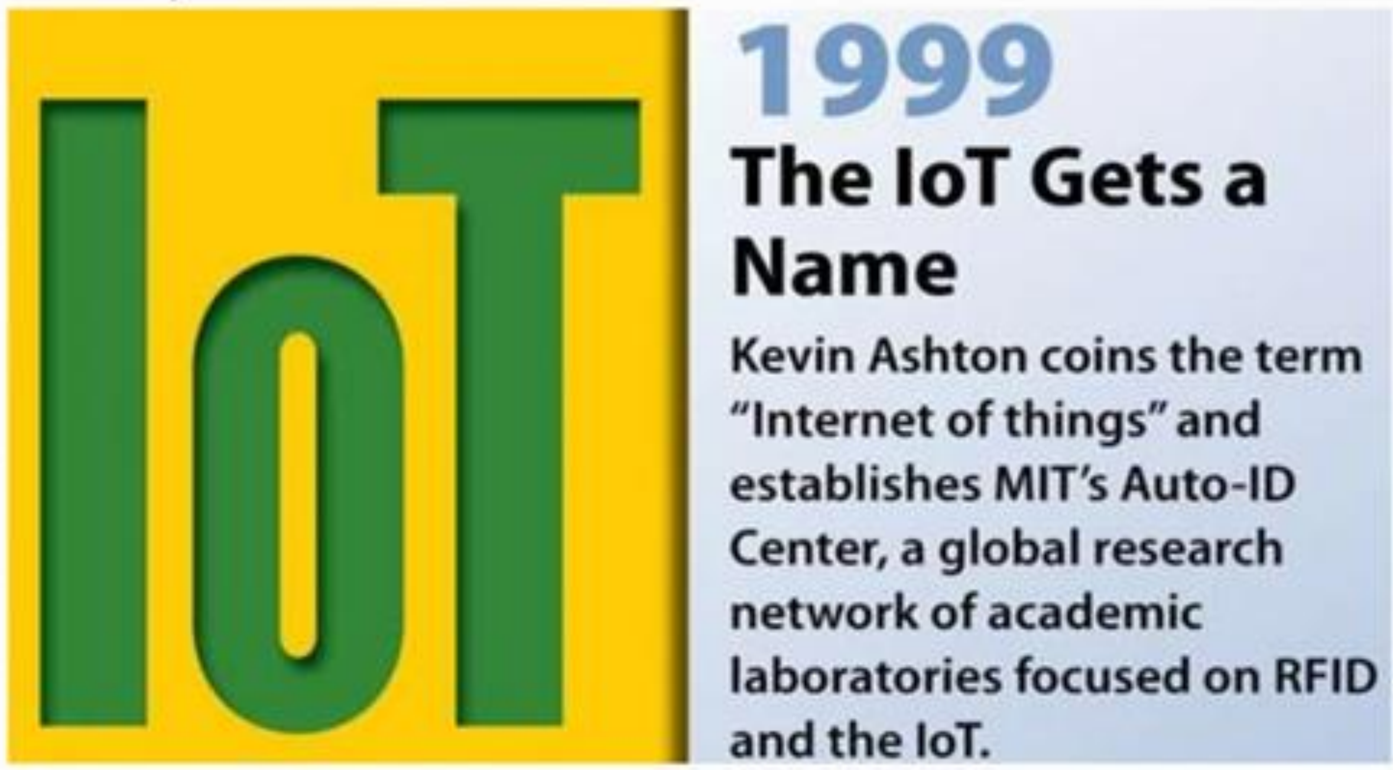
Nagaraju. Sonti

INTERNET of
THINGS

History of IOT

- 1999- The term "Internet of Things" was used by Kevin Ashton during his work at P&G which became widely accepted
- 2004 - The term was mentioned in famous publications like the Guardian, Boston Globe, and Scientific American
- 2005-UN's International Telecommunications Union (ITU) published its first report on this topic.
- 2008- The Internet of Things was born
- 2011- Gartner, the market research company, include "The Internet of Things" technology in their research

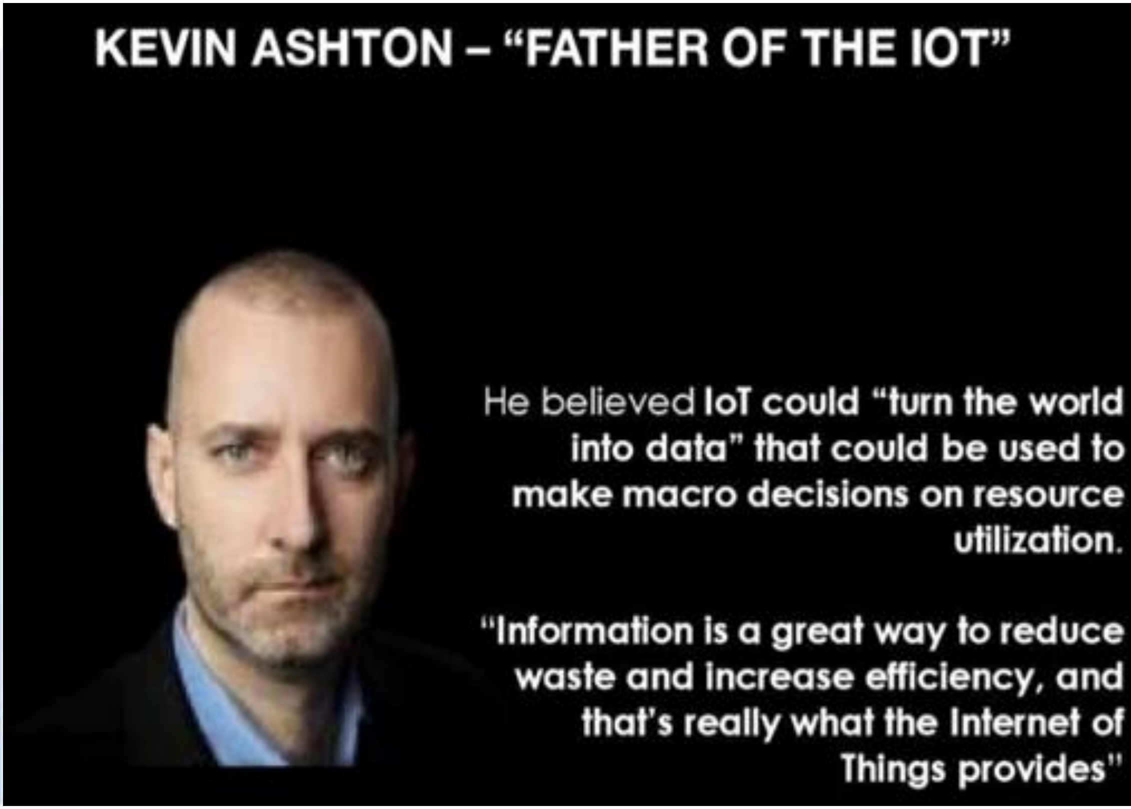
History of IoT



1999

The IoT Gets a Name

Kevin Ashton coins the term "Internet of things" and establishes MIT's Auto-ID Center, a global research network of academic laboratories focused on RFID and the IoT.



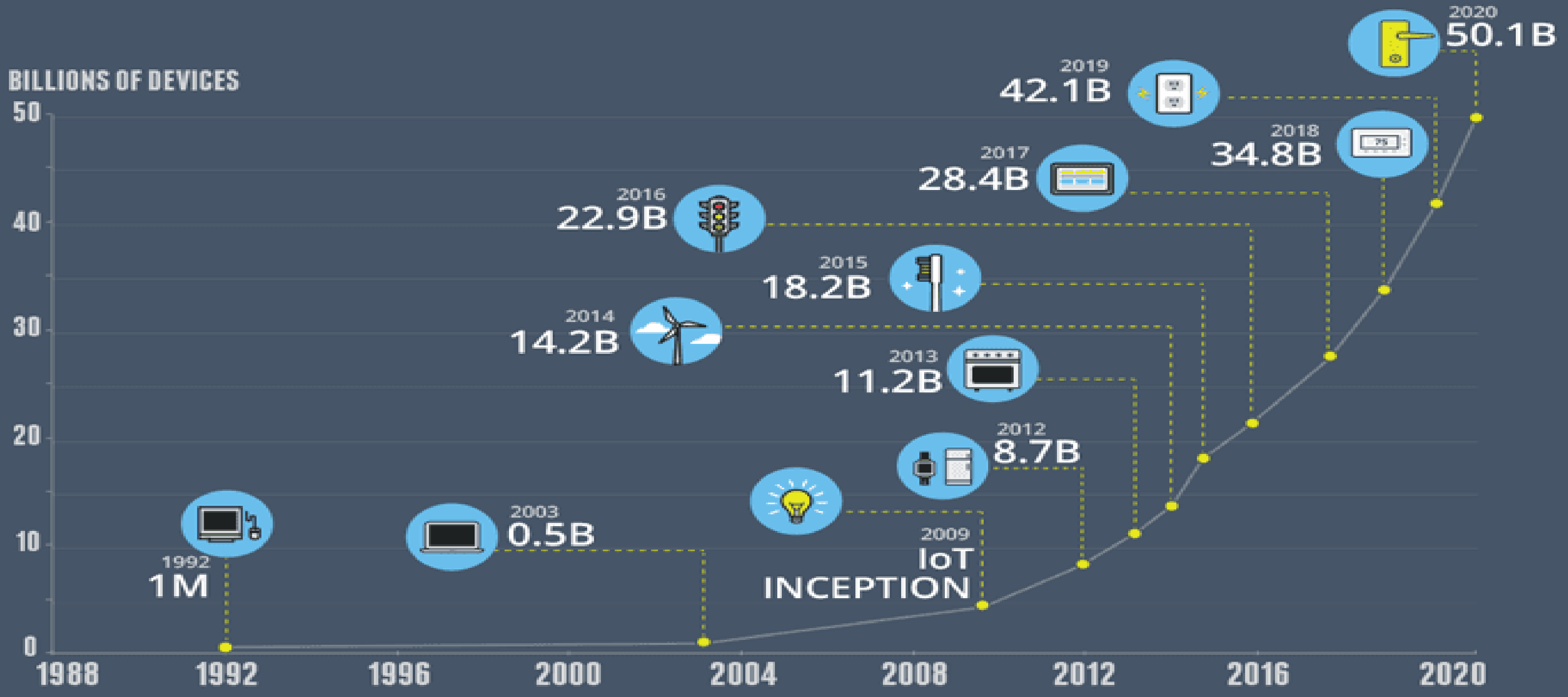
KEVIN ASHTON – "FATHER OF THE IOT"

He believed **IoT could "turn the world into data" that could be used to make macro decisions on resource utilization.**

"Information is a great way to reduce waste and increase efficiency, and that's really what the Internet of Things provides"

GROWTH IN THE INTERNET OF THINGS

THE NUMBER OF CONNECTED DEVICES WILL EXCEED 50 BILLION BY 2020



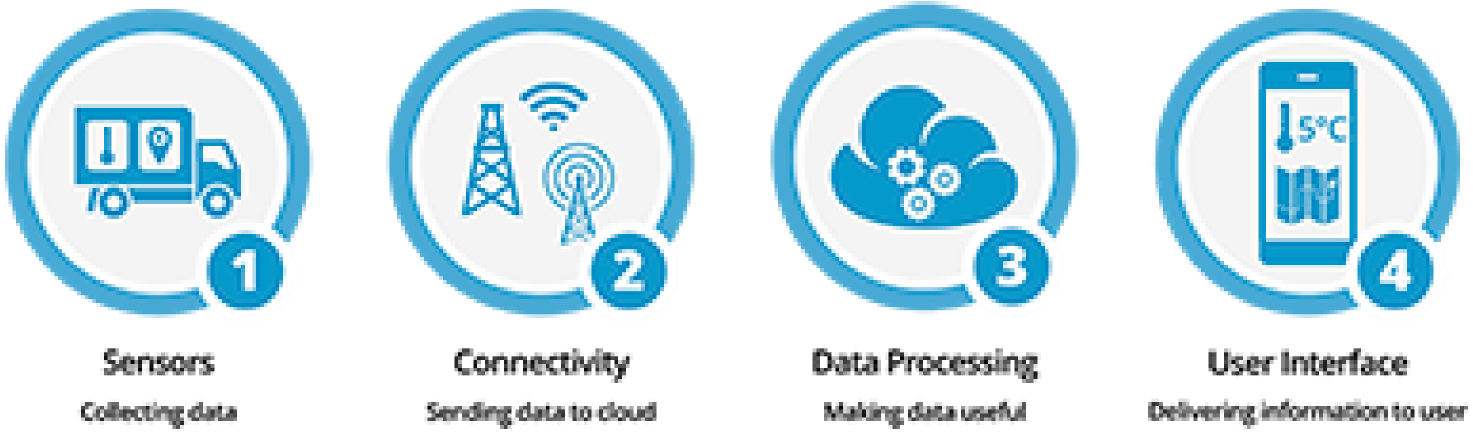
Source: Cisco

IoT Definition

- “The **Internet of Things** (**IoT**) is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.”

How IoT works?

- 1) Sensors/Devices
- 2) Connectivity
- 3) Data Processing
- 4)User Interface



1) Sensors/Devices

- Sensors or devices are a key component that helps you to collect live data from the surrounding environment.
- All this data may have various levels of complexities.
- It could be a simple temperature monitoring sensor, or it may be in the form of the video feed.

2) Connectivity

- All the collected data is sent to a cloud infrastructure.
- The sensors should be connected to the cloud using various mediums of communications.
- These communication mediums include mobile or satellite networks, Bluetooth, WI-FI, WAN, etc.

3) Data Processing

- Once that data is collected, and it gets to the cloud, the software performs processing on the gathered data.
- This process can be just checking the temperature, reading on devices like AC or heaters.
- However, it can sometimes also be very complex like identifying objects, using computer vision on video.

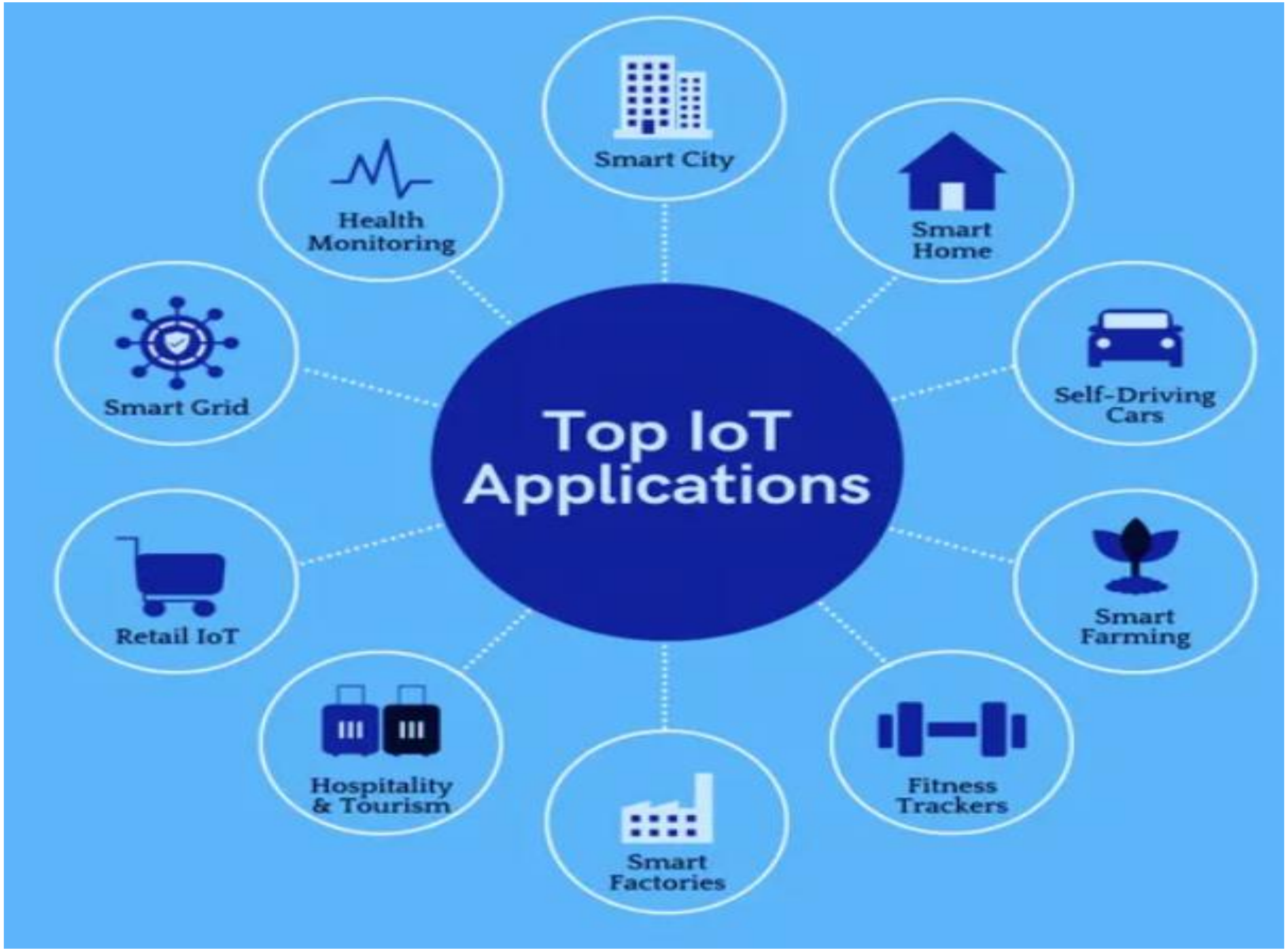
4)User Interface

- The information needs to be available to the end-user in some way which can be achieved by triggering alarms on their phones or sending them notification through email or text message.
- The user sometimes might need an interface which actively checks their IoT system.
- For example, the user has a camera installed in his home. He wants to access video recording and all the feeds with the help of a web server.

Why Is Internet of Things (IoT) so important?

- Over the past few years, IoT has become one of the most important technologies of the 21st century.
- Now that we can connect everyday objects—kitchen appliances, cars, thermostats, baby monitors—to the internet via embedded devices, seamless communication is possible between people, processes, and things.
- By means of low-cost computing, the cloud, big data, analytics, and mobile technologies, physical things can share and collect data with minimal human intervention.

IoT Applications



Advantages of IoT

- Ability to access information from anywhere at any time on any device;
- Improved communication between connected electronic devices;
- Transferring data packets over a connected network saving time and money; and
- Automating tasks helping to improve the quality of a business's services and reducing the need for human intervention.

Disadvantages IoT

- As the number of connected devices increases and more information is shared between devices, the potential that a hacker could steal confidential information also increases.
- Enterprises may eventually have to deal with massive numbers -- maybe even millions -- of IoT devices and collecting and managing the data from all those devices will be challenging.
- If there's a bug in the system, it's likely that every connected device will become corrupted.
- Since there's no international standard of compatibility for IoT, it's difficult for devices from different manufacturers to communicate with each other.

Characteristics of Internet of Things

- **According to the definition of internet of things (IoT), there are lot of IoT devices which are interconnected with each through internet. These devices sense the data continuously from their environment. Sensed data can either share with each other or transmitted on cloud server.**
- **IoT has various characteristics but most common are explained under, Major Characteristics of the Internet of Things**
- **The major characteristics of IoT as follows. Let’s discuss it one by one.**

1. Connectivity

2. Identity

3. Intelligence

4. Scalability

5. Dynamic and Self-Adapting

6. Architecture

7. Safety

1. Connectivity

- Connectivity is an important pillar of the IoT infrastructure. IoT devices should be connected regardless of their presence. Without connection, nothing makes sense.

2. Identity

- Each IoT device has its unique identity. If it needs to access the data from specific device, then its identification element is very helpful.

3. Intelligence

- The extraction of data from the sensor devices is very important. This data is only useful if it is interpreted properly. IoT perform operations on sensed data in such a way that the results are useful for us. It is the intelligence property of IoT.

4. Scalability

- The number of IoT devices are increasing day by day. Hence, the scalability of an IoT should be enough that it can handle the massive traffic.

5. Dynamic and Self-Adapting

- IoT devices should dynamically adapt themselves according to situations. For example, a camera can capture data according to light conditions. It is shifted to night or day mode automatically. It is self-Adapting technique.

6. Architecture

- IoT architecture should be hybrid, supporting different manufacturers. So, it cannot be homogeneous in nature. IoT is not the name of any engineering branch. IoT comes to picture when multiple domains come together.

7. Safety

- Safety should be the top priority. But in case of IoT, Safety is big challenge because multiple things are connected through internet. And security at each node is a critical and tough task.

Architecture of Internet of Things (IoT)

Architecture of Internet of Things (IoT)

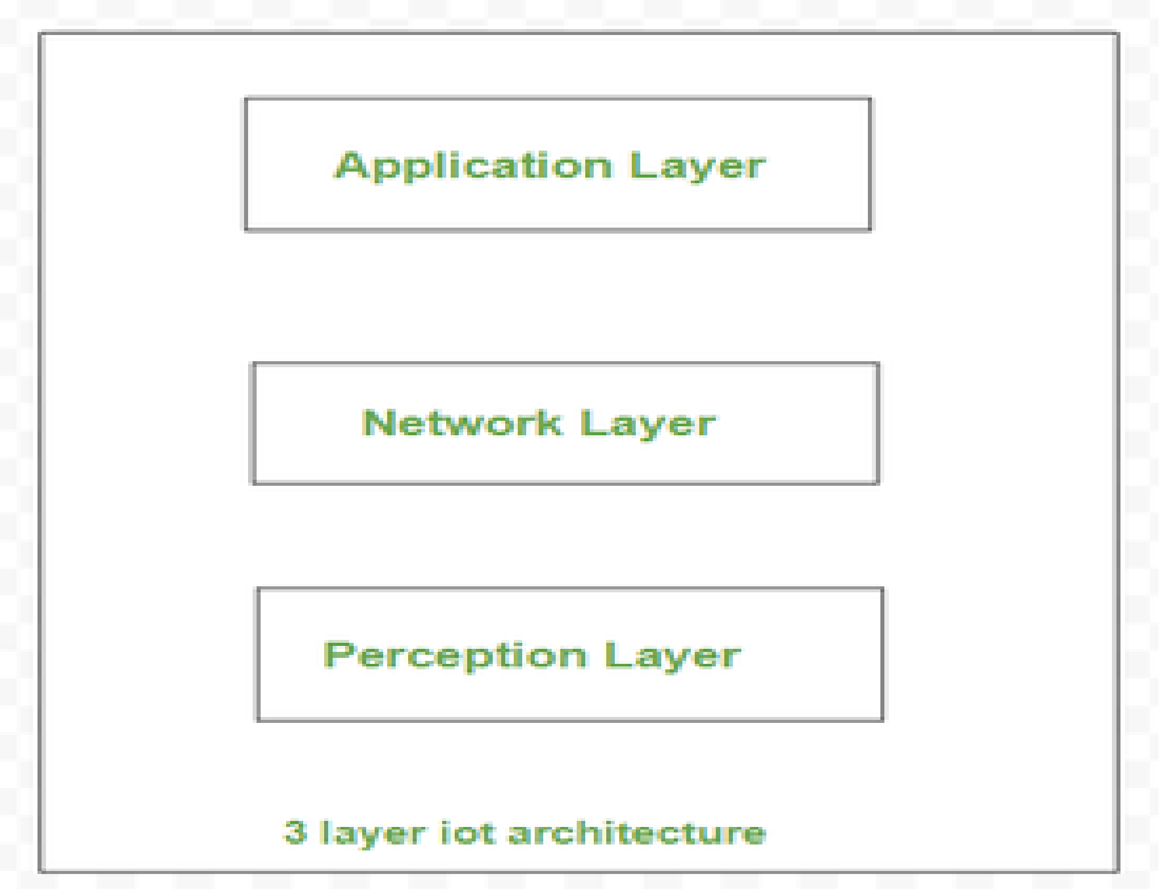
- Internet of Things (IoT) technology has a wide variety of applications and use of Internet of Things is growing so faster.

- Depending upon different application areas of Internet of Things, it works accordingly as per it has been designed/developed.

- it has not a standard defined architecture of working which is strictly followed universally.

- The architecture of IoT depends upon its functionality and implementation in different sectors.

3 layer IoT architecture :



Perception Layer :

- This perception layer is the IoT architecture’s physical layer. In these sensors and embedded systems are used mainly. These collect large amounts of data based on the requirements. This also includes edge devices, sensors, and actuators that communicate with the surroundings. It detects certain spatial parameters or detects other intelligent things /objects in the surroundings

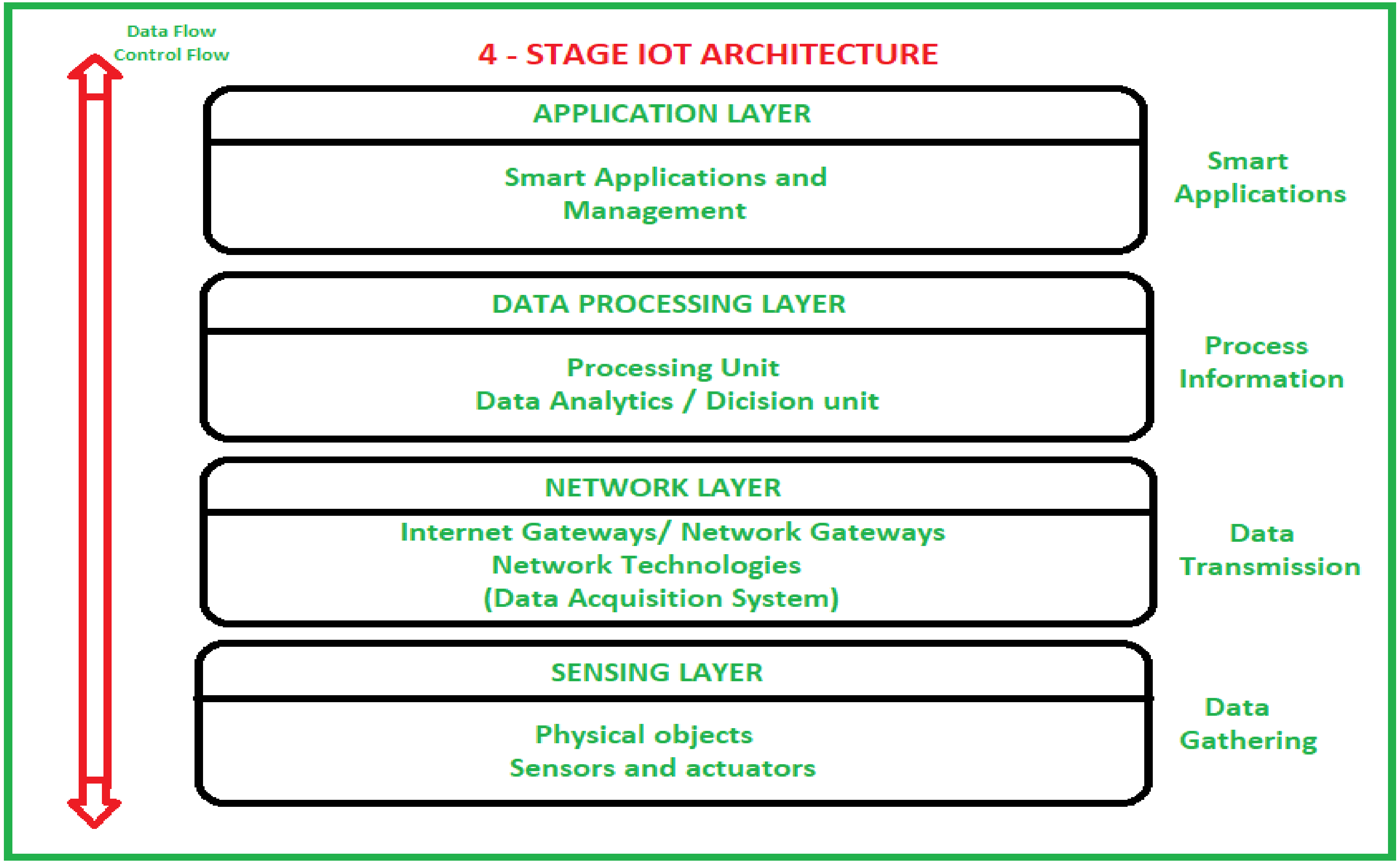
Network Layer :

- The data obtained by these devices must be distributed and stored. This is the responsibility of the network layer. It binds these intelligent objects to other intelligent/ smart objects. It is also in charge of data transfer. The network layer is in-charge of linking smart objects, network devices, and servers. Its is also used to distribute and analyze sensor data.

Application Layer :

- The user communicates with this application layer. It is in-charge of providing the customer with software resources. Example: in smart home application, where users press a button in the app to switch on a coffee machine, for example. The application layer is in-charge of providing the customer with application-specific resources. It specifies different uses for the IoT, such as smart houses, smart cities, and smart health.

Four Layered IoT architecture



Data Flow
Control Flow

4 - STAGE IOT ARCHITECTURE

APPLICATION LAYER

Smart Applications and Management

Smart Applications

DATA PROCESSING LAYER

Processing Unit
Data Analytics / Dicision unit

Process Information

NETWORK LAYER

Internet Gateways/ Network Gateways
Network Technologies
(Data Acquisition System)

Data Transmission

SENSING LAYER

Physical objects
Sensors and actuators

Data Gathering

Four Layered IoT architecture

- The 4 layers present in the architecture that can be divided as follows:

- Sensing Layer,
- Network Layer
- Data processing Layer
- Application Layer

Sensing Layer –

- Sensors, actuators, devices are present in this Sensing layer. These Sensors or Actuators accepts data(physical/environmental parameters), processes data and emits data over network.

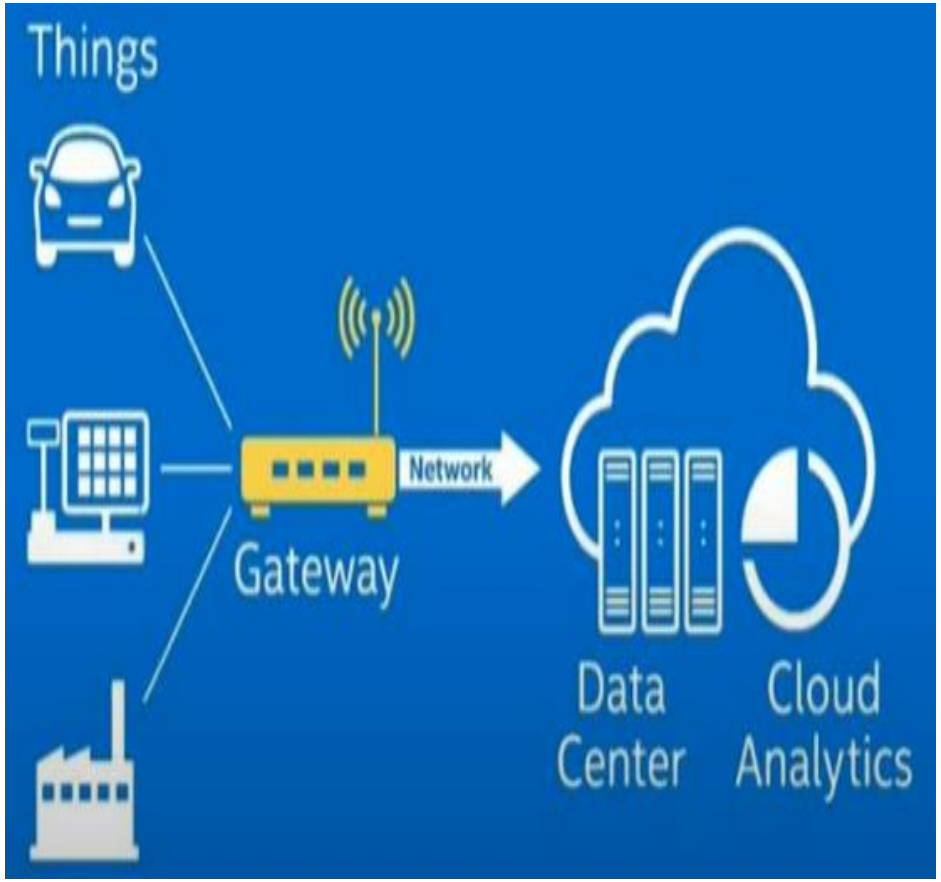
- Sensors collects data from the environment or object under measurement and turn it into useful data.

For example: Moisture sensor, Temperature sensor.

Network Layer –

Internet/Network gateways, Data Acquisition System (DAS) are present in this layer.

- The data from the sensors are in analog form. That data need to be aggregated and converted into digital form using DAS.
- The DAS connects to the sensor network , aggregates outputs, and performs the analog to digital conversion.
- The internet gateways receives the aggregated and digitized data and routes it over Wi-Fi, wired LANs, or the Internet , to the Third layer for further processing.



Data processing Layer –

- Pre-processing and enhanced analytics of the data is performed in the third stage of an IoT architecture. Edge IT systems are responsible for carrying out these tasks.

- IoT systems collect a significant amount of data and consequently require a lot of bandwidth, these Edge IT systems perform a vital task in reducing the load on the core IT infrastructure.

- Machine learning and visualization technologies are used by Edge IT systems to generate results from the collected data.

- Insights are provided by machine learning algorithms while the visualization technology presents the data in a way that's easy to understand.

Application Layer –

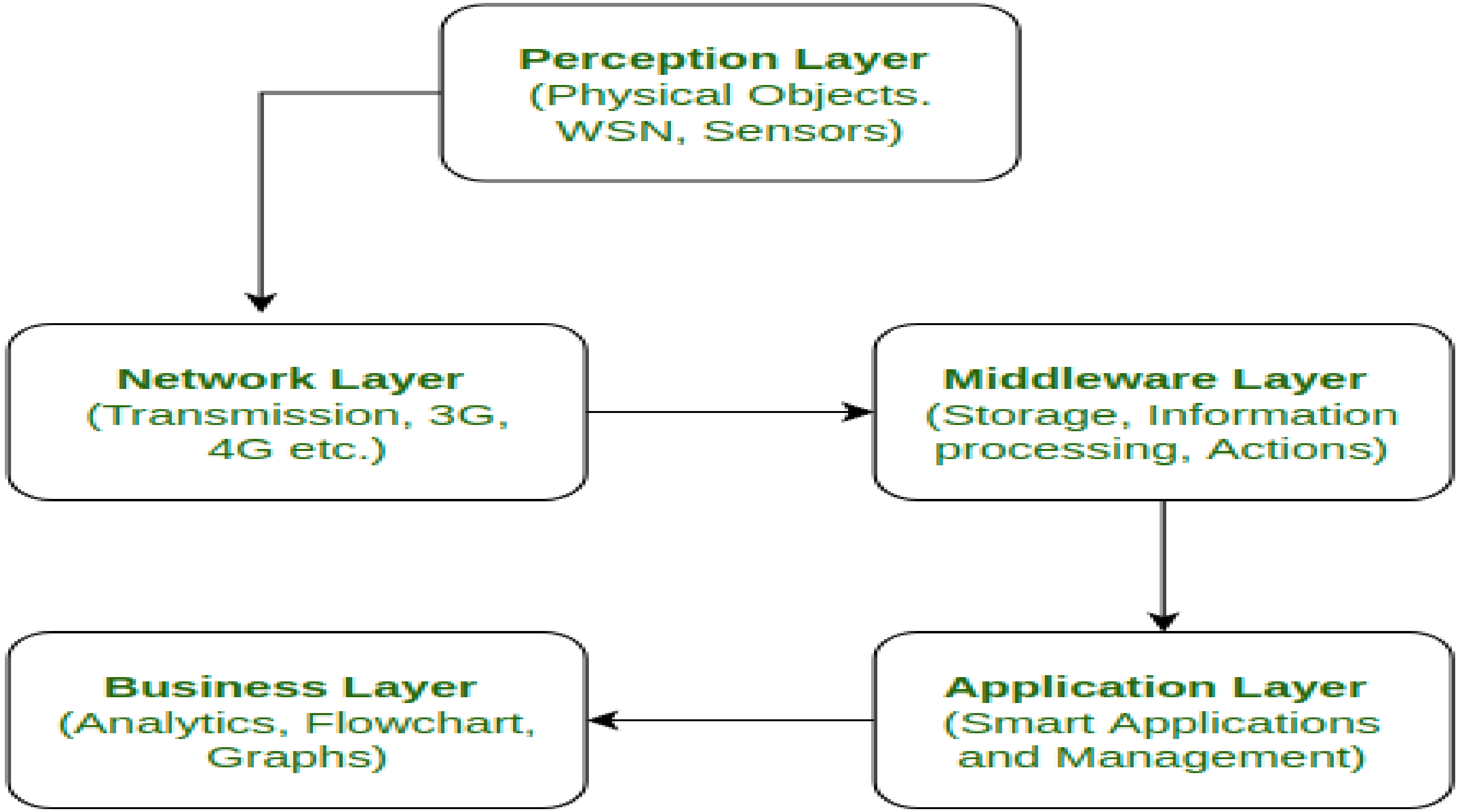
This is last layer of 4 stages of IoT architecture.

- The data needs to be stored for further in-depth analysis which is why data storage is such an important stage of an IoT architecture. It helps with follow-up revision for feedback as well. Cloud storage is the preferred storage method in IoT implementations.

- Data centers or cloud is management stage of data where data is managed and is used by end-user applications like agriculture, health care, aerospace, farming, defense, etc.

FIVE Layered Architecture of IoT:

- When project work is done with various cutting-edge technologies and broad application area, 5-layer architecture is considered as best.

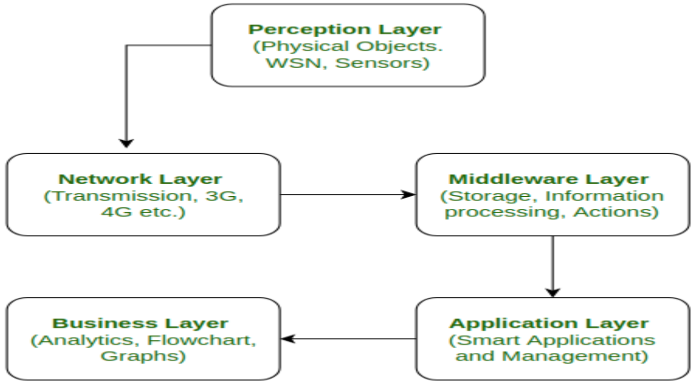


Perception Layer :

- This is the first layer of IoT architecture. In the perception layer, number of sensors and actuators are used to gather useful information like temperature, moisture content, intruder detection, sounds, etc.

- The main function of this layer is to get information from surroundings and to pass data to another layer so that some actions can be done based on that information.

Network Layer :


Perception Layer (Physical Objects. WSN, Sensors)
Network Layer (Transmission, 3G, 4G etc.)
Middleware Layer (Storage, Information processing, Actions)
Business Layer (Analytics, Flowchart, Graphs)
Application Layer (Smart Applications and Management)

- As the name suggests, it is the connecting layer between perception and middleware layer.
- It gets data from perception layer and passes data to middleware layer using networking technologies like 3G, 4G, UTMS, WiFI, infrared, etc.
- This is also called communication layer because it is responsible for communication between perception and middleware layer. All the transfer of data done securely keeping the obtained data confidential.

Middleware Layer:

- Middleware Layer has some advanced features like storage, computation, processing, action taking capabilities

- It stores all dataset and based on the device address and name it gives appropriate data to that device. It can also take decisions based on calculations done on dataset obtained from sensors.

Application Layer:

- The application layer manages all application process based on information obtained from middleware layer.

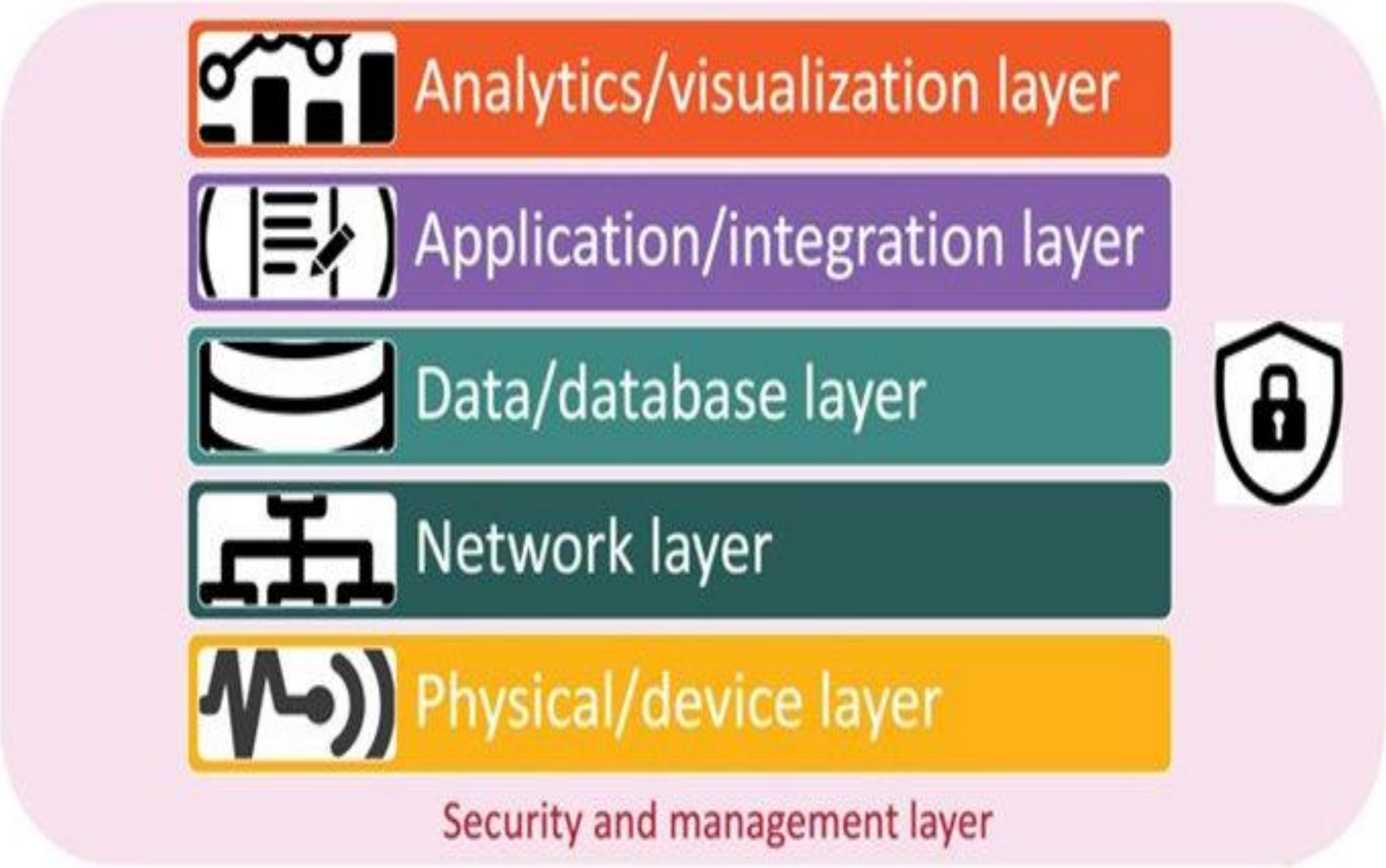
- This application involves sending emails, activating alarm, security system, turn on or off a device, smartwatch, smart agriculture, etc.

Business Layer:

- The success of any device does not depend only on technologies used in it but also how it is being delivered to its consumers. Business layer does these tasks for the device.

- It involves making flowcharts, graphs, analysis of results, and how device can be improved, etc.

Six Layered IoT architecture


Analytics/visualization layer
Application/integration layer
Data/database layer
Network layer
Physical/device layer
Security and management layer

Physical/device layer.

- This layer comprises the sensors, actuators and other smart devices and connected devices that comprise the physical layer and device layer.

- These smart devices either capture data (sensors), take action (actuators) or sometimes both

Network layer

- This layer comprises the network devices and communications types and protocols (5G, Wi-Fi, Bluetooth, etc.).

- Although many IoT architectures rely on general-purpose network layers, there is an increasing trend to move to dedicated IoT-specific networks.

Data/database layer.

- There are a range of databases used for IoT architectures, and many organizations spend a fair amount of time selecting and architecting the right IoT databases.

Analytics/visualization layer.

- This layer comprises the analytics layer, visualization layer and perception layer.

- This layer's focus is on analyzing the data provided by IoT and providing it to users and applications to make sense of.

Application/integration layer.

- This is the layer of applications and platforms that integrate together to deliver the functionality from the IoT infrastructure to the business.

- The processing layer and business layer are all part of the larger application/integration layer.

Security and management layer.

- This layer encompasses both the security layer and the management layer.
- This layer has connections with all the other layers to provide security and management. But it's an important component that's worth considering at every layer.

Challenges in Internet of things (IoT)

The main challenges and issues in IOT are

- Mobility
- Reliability
- Scalability
- Management
- Availability
- Interoperability

Mobility:

- Most of the IoT devices are mobile and hence they have a dynamic topology. Their IP address change based on the network and location. Routing protocols need to be adaptive to the changes in the network topology. If the mobility results in change of the service provider, the complexity further increases.

Reliability:

- IoT applications require devices to be more reliable and should respond to the changing environment rapidly and should communicate reliably. This is very crucial as a wrong information can lead to disastrous scenarios.

Scalability:

- The scalability is the biggest challenge in IoT network. As the number of connected devices in the network increases, managing the devices and their distribution becomes difficult. Accommodating services to the newly joined devices is also a tedious task.

Management:

- Management involves Faults, Configuration, Accounting, Performance and Security (FCAPS)aspects of all the devices.

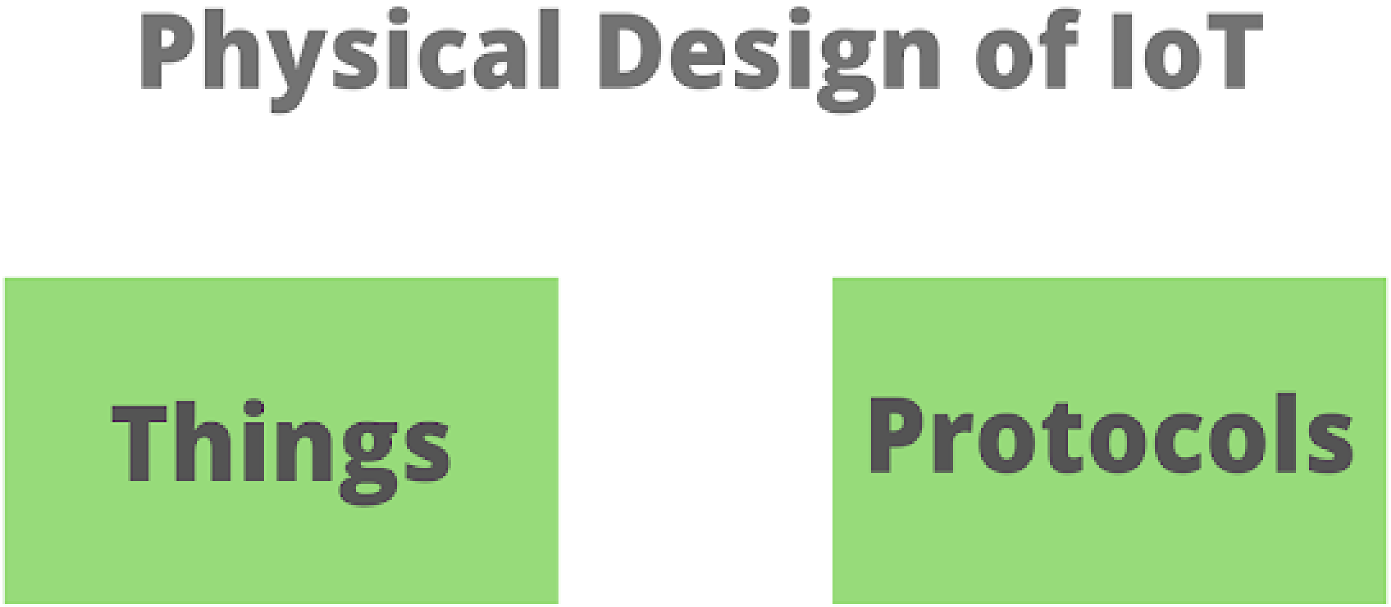
Availability:

- Availability is another factor of prime importance. The device should be available both in terms of software (services provided) and hardware (accessibility to other devices, compatibility with existing IoT functionalities and protocols)

Interoperability:

- Heterogeneity is the key attribute to the IoT network. With devices with different hardware platforms, operating systems, interoperability is the major issue of concern in IoT.

Physical Design of Internet of Things (IOT)



Physical Design of IoT

Things

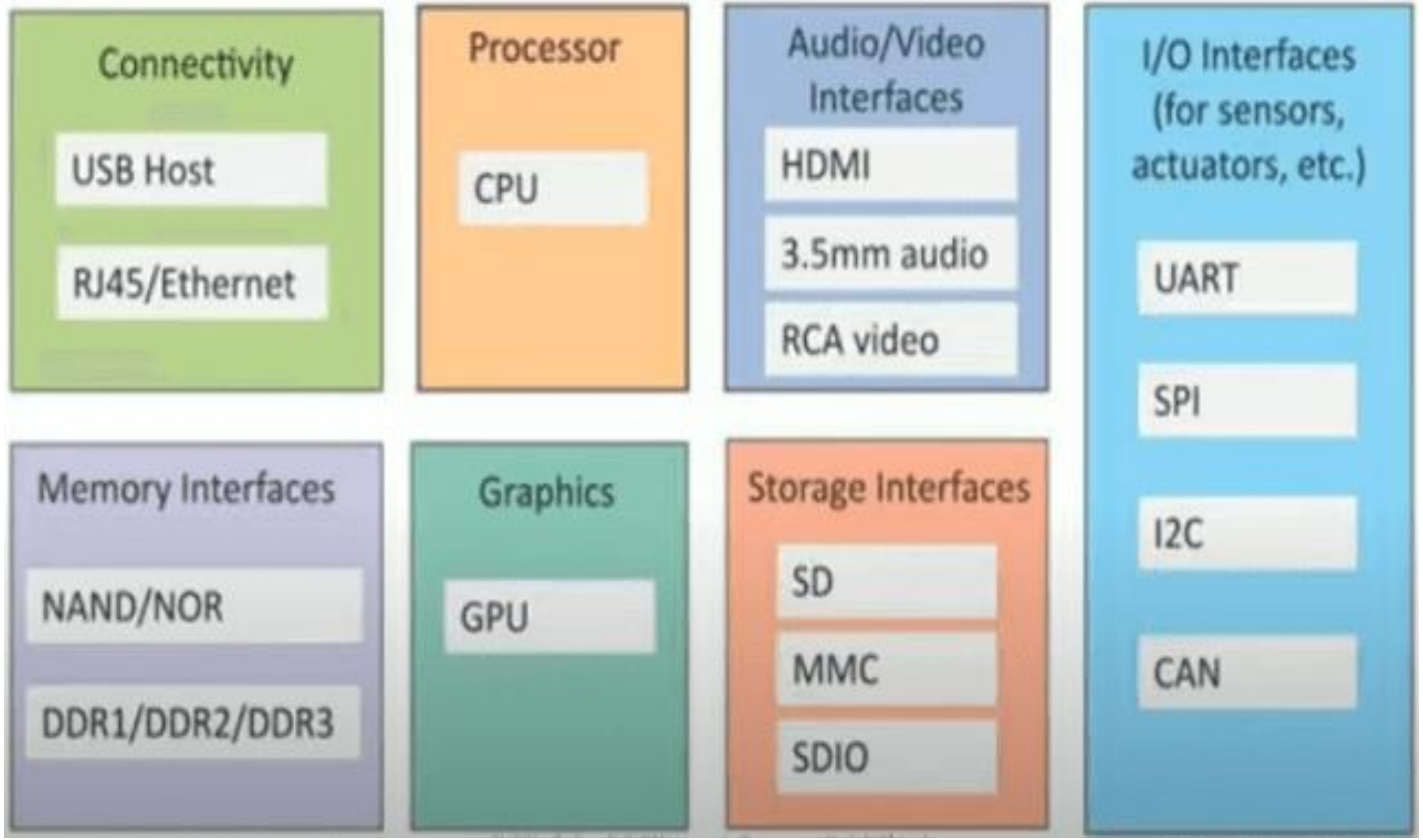
Protocols

Physical Design of Internet of Things (IOT)

- Things/Devices are called Node Devices and every device has a unique identity that performs remote sensing, actuating, and monitoring work.

- The protocols that are used to establish communication between the Node devices and servers over the internet.

Things/Devices



Connectivity

USB Host

RJ45/Ethernet

Processor

CPU

Audio/Video Interfaces

HDMI

3.5mm audio

RCA video

I/O Interfaces (for sensors, actuators, etc.)

UART

SPI

I2C

CAN

Memory Interfaces

NAND/NOR

DDR1/DDR2/DDR3

Graphics

GPU

Storage Interfaces

SD

MMC

SDIO

Connectivity

- Devices like USB hosts and ETHERNET are used for connectivity between the devices and the server.

Processor

- A processor like a CPU and other units are used to process the data. these data are further used to improve the decision quality of an IoT system.

Audio/Video Interfaces

- An interface like HDMI and RCA devices is used to record audio and videos in a system.

Input/Output interface

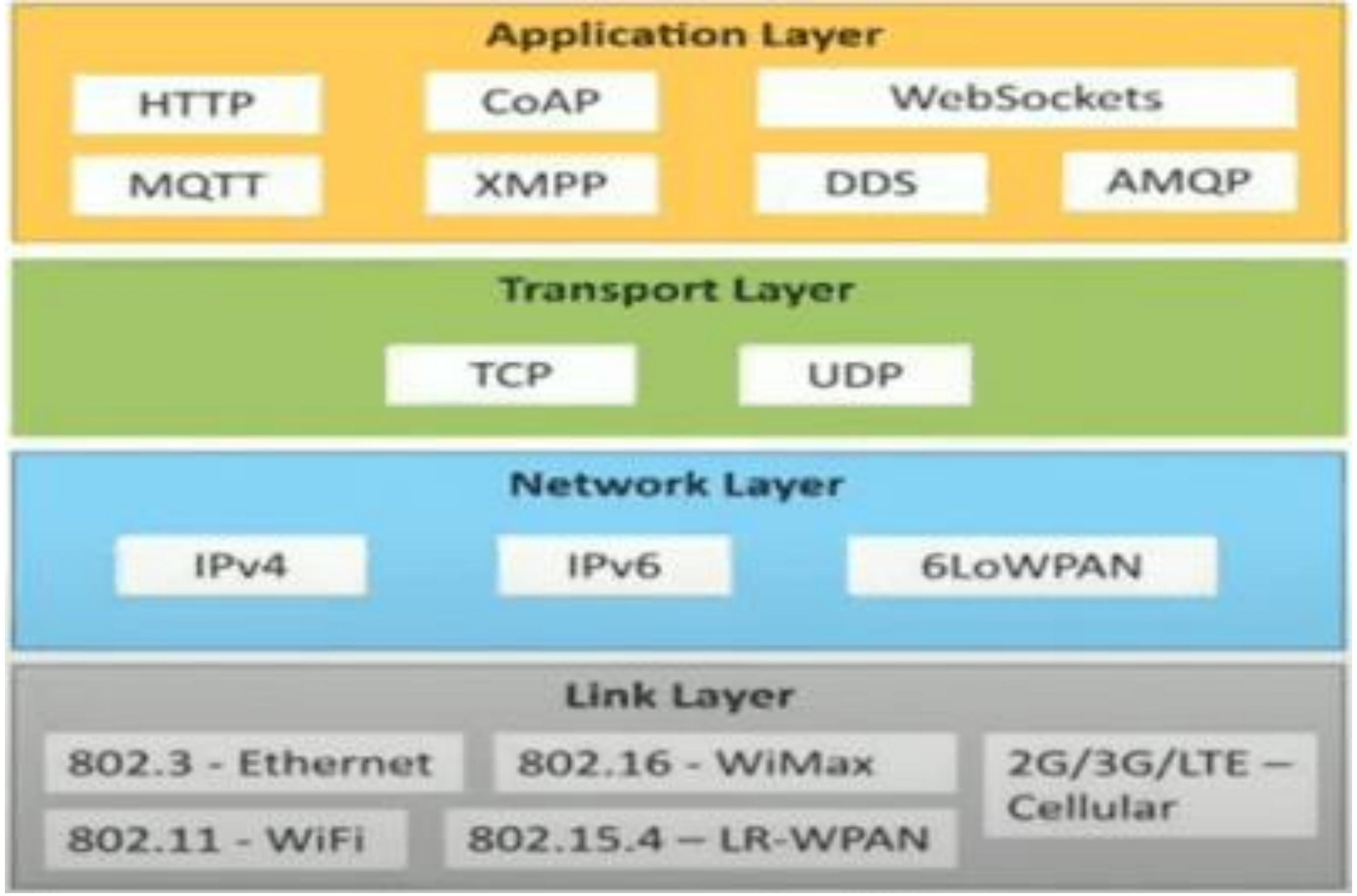
- To give input and output signals to sensors, and actuators we use things like UART, SPI, CAN, etc.

Storage Interfaces

- Things like SD, MMC, and SDIO are used to store the data generated from an IoT device.

- Other things like DDR and GPU are used to control the activity of an IoT system.

IoT Protocols



Application Layer

HTTP
CoAP
WebSockets
MQTT
XMPP
DDS
AMQP

Transport Layer

TCP
UDP

Network Layer

IPv4
IPv6
6LoWPAN

Link Layer

802.3 - Ethernet
802.16 - WiMax
2G/3G/LTE – Cellular
802.11 - WiFi
802.15.4 – LR-WPAN

Application Layer protocol

- In this layer, protocols define how the data can be sent over the network with the lower layer protocols using the application interface. these protocols include HTTP, WebSocket, XMPP, MQTT, DDS, and AMQP protocols.

HTTP

- Hypertext transfer protocol is a protocol that presents in an application layer for transmitting media documents.
- it is used to communicate between web browsers and servers.
- it makes a request to a server and then waits till it receives a response and in between the request server does not keep any data between two requests.

WebSocket

- This protocol enables two-way communication between a client and a host that can be run on an untrusted code in a controlled environment. this protocol is commonly used by web browsers.

MQTT

- Message Queuing Telemetry Transport is a lightweight messaging protocol. It uses publish-subscribe communication way and that’s why it is used for M2M (machine to machine) communication.
- It is based on TCP-IP protocol and is designed to operate in limited bandwidth. In the protocol terminology, the limited network bandwidth is referred as ‘small code footprint’.

Transport Layer protocol

- This layer is used to control the flow of data segments and handle the error control. also, these layer protocols provide end-to-end message transfer capability independent of the underlying network.

TCP

- The transmission control protocol is a protocol that defines how to establish and maintain a network that can exchange data in a proper manner using the internet protocol.
- It is suitable for reliable communication because in this protocol acknowledgment is received when the client sends the packet to the server via TCP protocol. The data must be guaranteed sent at the other end if the packet is sent via TCP protocol.
- The protocol operates in three phases – Connection establishment, data transfer and connection close. A TCP connection is managed by an internet socket which lying at the end point (physical) undergoes various state changes.

UDP

- User Datagram Protocol is a connection less protocol and is not reliable for guaranteed transmission of data.
- UDP protocol is a best protocol to send data to the server when packet loss during transmission of the data can be afforded.
- UDP protocol is a lightweight protocol and is suitable for wireless sensor network communication. UDP is often used in applications specially tuned for real-time performance.

Network Layer protocol

- This layer is used to send datagrams from the source network to the destination network. we use IPv4 and IPv6 protocols as host identification that transfers data in packets.

IPv4

- This is a protocol address that is a unique and numerical label assigned to each device connected to the network.
- IPv4 addresses are expressed as dotted decimal numbers. The address consist of four octets (32-bit number) divided into two parts – network address to uniquely identify a TCP-IP or IOT network and host address to identify host within the identified network.
- A subnet mask is used along with the 32-bit IP address to uniquely identify a host (computer or IOT device). The subnet mask helps in identifying the exact location of the host device. The routers extract the network address from the IPv4 address and compare it with a route table to identify the network and the data packet is first delivered to the target network. Then, the subnet mask is used to uniquely identify the host and deliver the data packet to the host device.

IPv6

- It is a successor of IPv4 that uses 128 bits for an IP address.
- The address space in IPv4 is limited to roughly 4.3 billion devices. There will be 20 billion IOT devices alone by the year 2020. So, an IP addressing standard that would be scalable to cater to the future IOT infrastructure was the need of the time.
- Compared to 32-bit addresses in IPv4, there are 128-bit addresses in IPv6. The address is divided into eight 16-bit blocks where each block can be represented by a 4-digit hexadecimal number. each block in the IPv6 address is separated by a semi-colon. So, a typical IPv6 address would look like 77AD:45DF:A23D:8:2D:76DF:245:AF. There are eight blocks in the address – 77AD, 45DF, A23D, 8, 2D, 76DF, 245 and AF.

6LoWPAN

- IPv6 Low Power Wireless Personal Area Network (6LoWPAN) is an IPv6 standard based network layer protocol for Wireless Personal Area Networks.
- This protocol is a modified version of IPv6 with intention to implement Internet protocol to each and every devices (constrained devices as well as large devices) and the low power devices with limited capabilities like less memory, lossy network etc.
- 6LoWPAN networks connect to the Internet via a gateway (WiFi or Ethernet), which does some process for protocol conversion so that device can communicate with Internet.

Link Layer protocol

- Link-layer protocols are used to send data over the network's physical layer. it also determines how the packets are coded and signaled by the devices.

Link Layer Protocols:

	Ethernet	Wifi	WiMax	LR-WPAN	LTE
About	• Collection of wired Ethernet standard • Standard for 10BASEE5 Ethernet	- Collection of wireless LAN (WLAN)	Collection of wireless broadband standards	•Collection of standard low rate wireless personal area networks (LR- WPANS) •Forms the basis for high level communication protocols -> zigbee	-Different generations of mobile communication standards
Variants	•802.3.i 10BASE-T copper twisted pair •802.3.j 10BASE-F fibre Optic •802.3.ae:10GB/Ethernet over fibre	•802.11a (5Hz) •802.11b(2.4 GHz) •802.11g(2.4) •802.11n (2.4/5 GHz) •802.11ac(5 GHz) •802.11ad (60GHz)			2G: GSM/CDMA 3G:UMTS 4G:LTE
Data Rate	10Mb/s to 40Gb/s	1Mb/s to 6.75 Gb/s	1.5 Mb/s to 1 Gb/s	40Kb/s to 250 Kb/s	2G: 9.6Kb/s Upto 4G:100 Mb/s

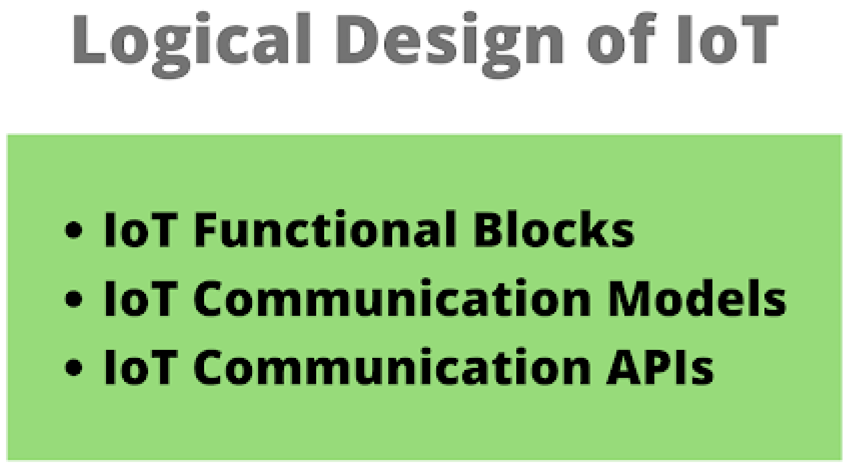
Ethernet

- It is a set of technologies and protocols that are used primarily in LANs.
- It is based on IEEE 802.3 standard. Within an IOT system, Ethernet can be used to connect stationary or fixed IOT devices. Like, it can be used to connect sensor networks in an industry, appliance control circuits in a home automation system or IOT devices in an office automation system.

WiFi

- WiFi is a local area network which is a wireless network there is no wired connection. It is Proposed by Wi-Fi Alliance.
- WiFi provides Internet access to devices within a range of 60 feet to 100 feet. It uses high-frequency radio signals for sending and receiving data.
- It uses the IEEE 802.11 standard. Its data rate varies from 2Mbps to 1.73Gbps.

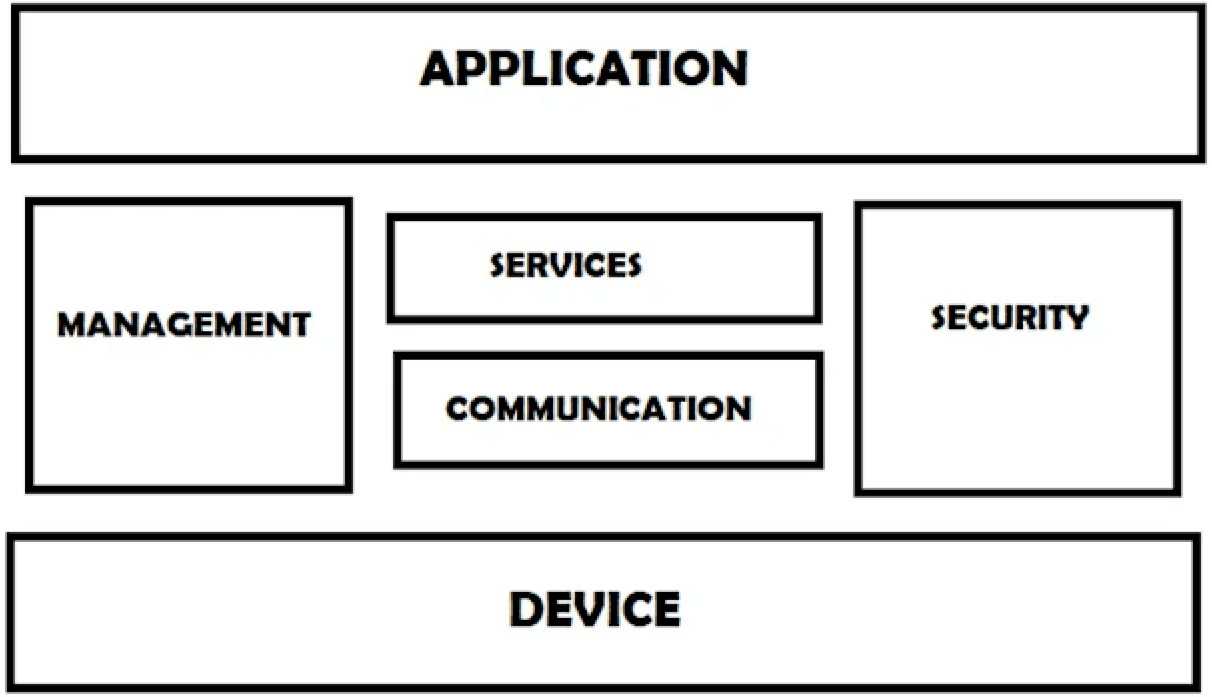
Logical Design IOT



Logical Design of IoT

- IoT Functional Blocks
- IoT Communication Models
- IoT Communication APIs

IoT Functional blocks



Devices

- provides sensing and monitoring control functions that collect data from the outer environment.

- Application

It is an interface that provides a control system that use by users to view the status and analyze of system.

- Management

This functional block provides various functions that are used to manage an IoT system.

- Services

This functional block provides some services like monitoring and controlling a device and publishing and deleting the data and restoring the system.

- Communication

This block handles the communication between the client and the cloud-based server and sends/receives the data using protocols.

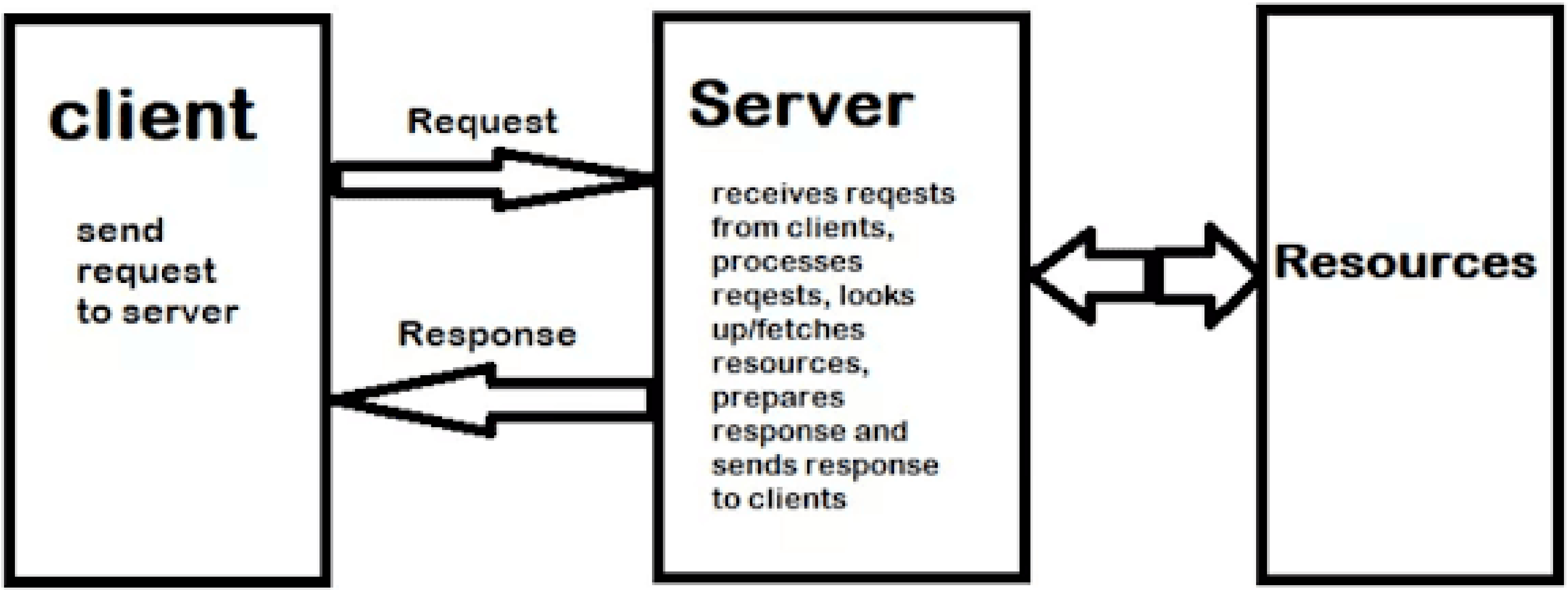
- Security

This block is used to secure an IoT system using some functions like authorization, data security, authentication, 2-step verification, etc.

IoT Communication Models

- There are several different types of models available in an IoT system that is used to communicate between the system and server like the request-response model, publish-subscribe model, push-pull model, exclusive pair model, etc.

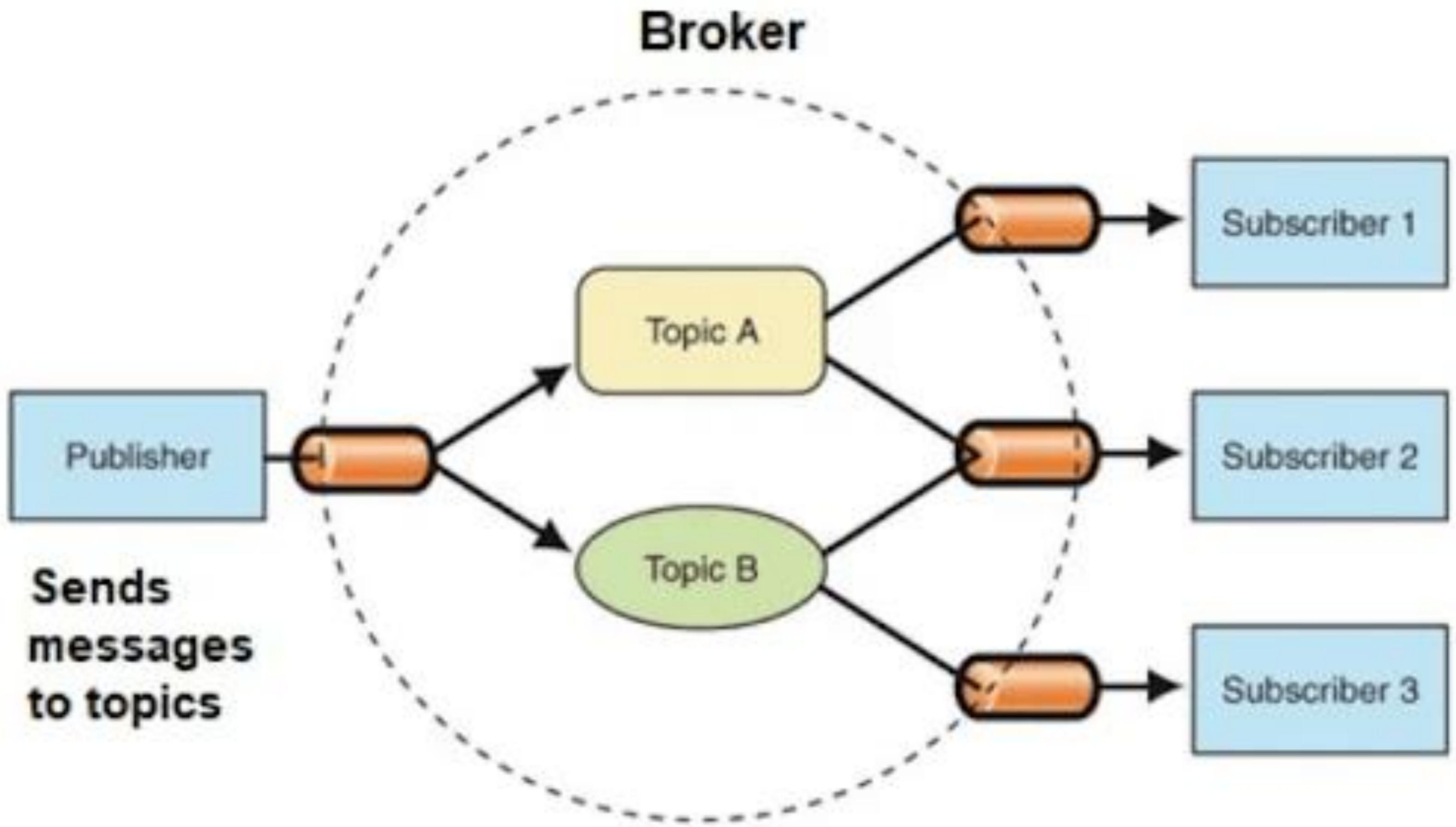
Request-Response Communication Model



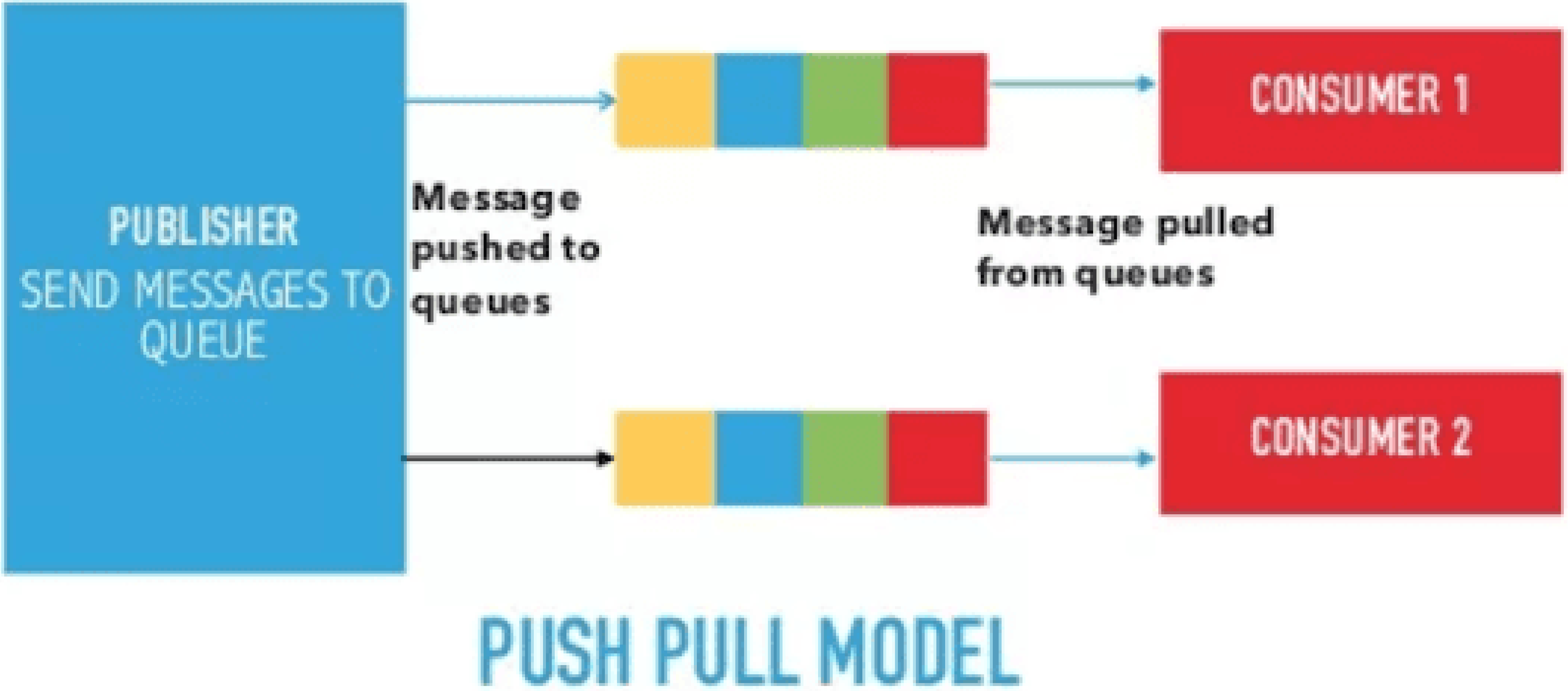
client
send request to server
Request
Response
Server
receives reqests from clients, processes reqests, looks up/fetches resources, prepares response and sends response to clients
Resources

Request-Response Communication Model

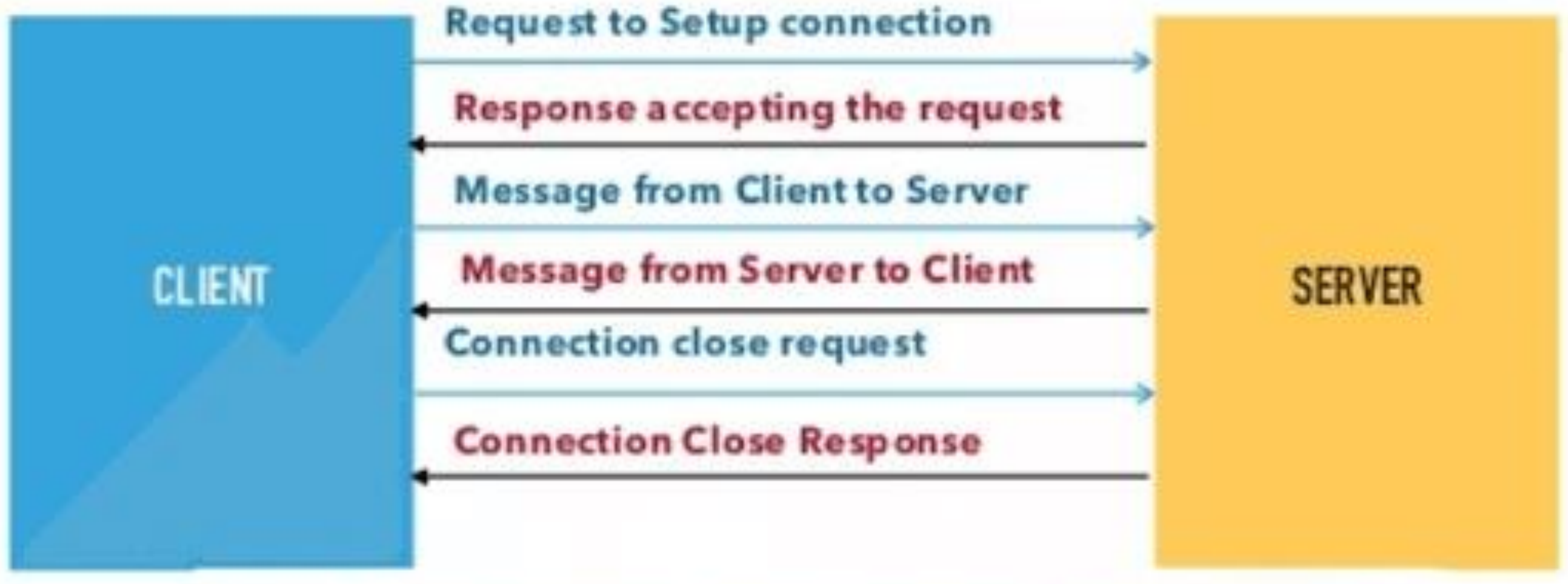
Publish-Subscribe Communication Model



Push-Pull Communication Model



Exclusive Pair Communication Model


Request to Setup connection
Response accepting the request
Message from Client to Server
Message from Server to Client
Connection close request
Connection Close Response
CLIENT
SERVER

EXCLUSIVE PAIR COMMUNICATION MODEL

IoT communication APIs

- These APIs like REST and WebSocket are used to communicate between the server and system in IoT.

REST-based communication APIs

- Representational state transfer(REST) API uses a set of architectural principles that used to design web services. these APIs focus on the systems' resources that how resource states are transferred using the request-response communication model.

- Client-server

Here the client is not aware of the storage of data because it is concerned about the server and similarly the server should not be concerned about the user interface because it is a concern of the client. and this separation is needed for independent development and updating of server and client. no matter how the client is using the response of the server and no matter how the server is using the request of the client.

- Stateless

It means each request from the client to the server must contain all the necessary information to understand by the server. because if the server can't understand the request of the client, then it can't fetch the request data in a proper manner.

Cacheable

- In response, if the cache constraints are given then a client can reuse that response in a later request. it improves the efficiency and scalability of the system without loading the extra data.

WebSocket based communication API

- This type of API allows bi-directional full-duplex communication between server and client using the exclusive pair communication model.
- This API uses full-duplex communication, so it does not require a new connection setup every time when it requests new data.
- WebSocket API begins with a connection setup between the server and client and if the WebSocket is supported by the server then it responds back to the client with the successful response after the setup of a connection server and the client can send data to each other in full-duplex mode.
- This type of API reduces the traffic and latency of data and makes sure that each time when we request new data it cannot terminate the request.